Part A: Office of the Secretary
Chapter AB: Deputy Secretary
Chapter ABE: Office of Security and Strategic Information

Part A: Office of the Secretary
Chapter AB: Deputy Secretary
Chapter ABE: Office of Security and Strategic Information

[1]Approved by the Assistant Secretary for Administration and Management on 11/21/2002 and published @ 67 FR 71568-70, dated 12/2/2002; [2]Approved by the Secretary on 4/3/2007 and published @72 FR 19000-01 on April 16, 2007

Office of Security and Strategic Information (ABE)
ABE.00 Mission
ABE.10 Organization
ABE.20 Function

Section ABE.00 Mission. On behalf of the Secretary and the Deputy Secretary, the Office of Security and Strategic Information (OSSI) provides broad Department-wide policy direction, standards setting, coordination, and performance assessment for organizational components within HHS in the areas of: physical security; personnel security and suitability; security awareness; information security, including the safeguarding of classified material and classification management; communication security; security and threat assessments; and strategic information programs and activities. OSSI functions as a platform to further HHS' roles in its various missions for protecting and improving the public health of the Nation, by protecting employees and visitors and Departmentally owned and occupied critical infrastructure, and by assuring the integration of strategic medical, public health, biomedical, and national security information. OSSI engages in and manages multiple internal Department and external relationships with other Federal Government Departments and agencies and external constituencies. OSSI directly manages and administers the flow of classified information and provides national security information services to all components within the Office of the Secretary (OS).

Section ABE.10 Organization. The Office of Security and Strategic Information (ABE) is headed by a Director who reports directly to the Deputy Secretary, and includes the following components:

- Immediate Office (ABE)
- Division of Physical Security (ABE1)
- Division of Personnel and Classified Information Security (ABE2)
- Division of Strategic Information (ABE3)

Section ABE.20 Functions.

1. **Immediate Office (ABE)**. The Immediate Office of the OSSI is responsible for the

following: (1) Providing overall leadership for the development, coordination, application, and evaluation of all policies and activities within the Department that relate to physical and personnel security, the security of classified information, and the exchange and coordination of national security-related strategic information with our Federal Government Departments and agencies and the national security community, including national security-related relationships with law enforcement organizations (LEOs) and public safety agencies; (2) serving as the principal advisor to and representative of the Secretary and Deputy Secretary on national security, physical and personnel security, security awareness, classified information security, and related medical, public health, and biomedical strategic information matters, including with organizations outside of the Department; (3) directing activities for all committees and work groups pertaining to these matters; (4) serving as the manager for any designation of representatives to external national security and related work groups; (5) providing policy oversight and coordination related to the architectural security function in the Office of the Assistant Secretary for Administration and Management (ASAM); the Cyber security and critical infrastructure functions in the Office of the Assistant Secretary for Resources and Technology (ASRT); and the Select Agents Program within the Centers for Disease Control and Prevention (CDC) and other Departmental units having select agent responsibilities; (6) serving as the principal contact with the Office of the Director of national Intelligence, and all of its subsidiary organizations; (7) serving as the principal contact point for other Federal Government Departments and agencies that have an interest in the sharing of strategic or national security-related medical, public health, and related scientific information; (8) approving the detail or assignment of personnel to or from components of national security agencies, LEO, and public safety agency communities, and serving as supervisor during their term (9) working with the Office of the Inspector General and the Office of the Assistant Secretary for Preparedness and Response (ASPR) on issues of mutual interest; and (10) conducting periodic assessments of the performance of relevant systems and activities and providing reports and recommendations to the Secretary and Deputy Secretary.

2. **Division of Physical Security (ABE1)**. The Division of Physical Security (DPS) is responsible for the following: (1) Providing policy guidance, setting standards, and overseeing all matters pertaining to: (a) The physical security of facilities, stockpiles, vendor-managed inventories, logistical systems, employees, visitors, and contractors; (b) security functions during disaster and emergency response, including those at principal and alternate emergency operations locations, and providing assistance to and coordination with the ASPR for deployed HHS personnel, resources, and activities; (c) security and force protection during emergency activities, including by working with military and civilian Federal Government Departments and agencies, State, and local LEOs and public safety agencies; (d) physical security components of Homeland Security Presidential Directives, as well as similar Directives or Executive Orders on national security matters; (2) representing the Department at the Interagency Security Committee, Information Sharing Council, and other similar committees and work groups; (3) coordinating

with the ASRT on matters pertaining to policies for Cyber protections, the National Cyber Security Response Program, and the Critical Infrastructure Assurance Program and with the ASAM on policies pertaining to the architectural security program, and conducting periodic collaborative reviews of these programs; (4) serving as the day-to-day point of contact with local, State, and Federal LEOs and public safety agencies on OSSI-related subject matter; (5) coordinating activities with the Secretary's Operations Center, when appropriate; and for (6) coordinating and overseeing the Department's internal critical infrastructure protection program.

3. **Division of Personnel and Classified Information Security (ABE2)**. The Division of Personnel and Classified Information Security (DPCIS) is responsible for the following: (1) Providing policy guidance, setting standards, and overseeing all matters pertaining to: (a) Personnel security, national security clearances, and suitability programs as they apply to Departmental employees, consultants, and contractors; (b) communications security, including the integrity of classified information systems, technology, terminals and databases, and telecommunications security, and for direct management of these functions for all organizational elements contained within the OS; (2) establishing policies for and directing the Department's drug-free workplace program; (3) initiating and conducting national security clearance processes and background investigations for Departmental employees, consultants, or contractors, and maintaining related records; (4) establishing Department-wide policies and awareness programs for information security to include the control of classified and sensitive but unclassified (SBU) materials, secure information handling and storage, and related training programs; (5) coordinating national security clearance interchange between Federal Government Departments and agencies and other organizations; (6) directing a Department-wide international traveler training and awareness program and foreign visitor awareness program; (7) within the OS, headquarters facilities, and continuity sites, directly managing classified materials, access to sensitive compartmented information facilities 9SCIFs) and information storage areas, secure audio and video systems, and other classified and secure communications systems; (8) establishing and overseeing Department-wide policies for similar functions and resources within the Department; (9) establishing and overseeing Department-wide policies for document classification management; and for (10) establishing standards to ensure awareness of appropriate practices to safeguard confidential and classified information held by the Department.

4. **Division of Strategic Information (ABE3**). The Division of Strategic Information (DSI) is responsible for the following: (1) Establishing policies and procedures to share and convey sensitive and classified information to users in the Department; (2) receiving, assessing, and evaluating products, reports, and other strategic information for applicability in the context of the various public health and science missions of the Department; (3) providing briefings, digests, and science-based reviews and assessments related to strategic and classified information; (4) controlling the flow of mission-driven sensitive, classified, and strategic

information within OS, and coordinating the flow between other components of the Department; (5) coordinating and superintending the flow of strategic national security-related public health and science information to and from HHS personnel detailed or assigned to national security agencies, LEOs, and public safety agencies; (6) managing and providing liaison for open source information programs and workgroups and the Information Sharing Environment Council; (7) providing policy direction for procedures to facilitate the identification of circumstances that are a potential vulnerability or threat to security; (8) conducting analyses of potential or identified risks to security and safety and working with agencies to develop methods to address them, including assisting in program implementation, performance evaluation, and oversight; and for (9) promoting cross-agency and inter-Departmental information sharing and scientific analysis collaborations.